Information Security Managers Group
Thursday, May 27, 2010 Meeting Minutes

MEETING LOGISTICS (all meeting minutes are posted on the ISMG Sharepoint site:
http://ent.sharepoint.mt.gov/groups/ism/default.aspx)

When: Last Thursday of each month 1:00 pm – 2:30 pm
Who: Agency CIO and/or Information Security Manager
Where: Department of Labor and Industry First Floor Conference Room
Corner of Lockey and Sanders
Next Meeting: Tentative – June 24, 2010 1:00 pm

PRESENT

MDT: Kristi Antosh
DLI: Judy Kelly
DOC: Larry Krause
DOA: Kevin Winegardner - Chair
OPI: Jim Gietzen for Joan Anderson
HHS: Chris Silvonen for Jacklynn Thiel

PURPOSE

The Information Security Managers Group has three primary purposes:

- Advise the State CIO on Information Risk Management Issues at the Statewide level
- Raise awareness while identifying communities of interest for EPP purposes
- Provide a forum for agency exchange of information

AGENDA ITEMS

- **Welcome and (re)introductions**
  - The Group members introduced themselves around the table.

- **Training on NIST Controls – Control Family – Program Management Control PM-1 = Security Program Plan**
  - Discussion:
    - Chair presented and explained NIST Control Family "Program Management", (see document NIST Program Management Control Family.docx located here: http://ent.sharepoint.mt.gov/groups/ism/irmp/Planning/Forms/AllItems.aspx?RootFolder=%2fgroups%2fism%2firmp%2fPlanning%2fISRMP%20Plan&FolderCTID=&View=%7b9FBC1CC6%2dA447%2d4B8F%2d8F78%2d2B1E6E645E87%7d

- **Review Key Elements of an Information Security Program**
  - Discussion:
    - The group reviewed and discussed key program elements and reviewed possible outline of the elements of an Information Security Program Plan. See sample Information Security Program Plan outline based on NIST PM-1 control here: http://ent.sharepoint.mt.gov/groups/ism/irmp/Planning/Forms/AllItems.aspx?RootFolder=%2fgroups%2fism%2firmp%2fPlanning%2fISRMP%20Plan&FolderCTID=&View=%7b9FBC1CC6%2dA447%2d4B8F%2d8F78%2d2B1E6E645E87%7d

        - The group discussed and recognized that to achieve the Goal of the Program Plan, multiple Objectives would be necessary. Additionally, each Objective could require one or more Tasks be accomplished to achieve an individual Objective.
        - The group also agreed that a "Program" (plan Goal), was normally implemented by the identification of specific key components (plan Objectives/Tasks), and that these components could be delivered/implemented by specific "Projects" (and possibly sub-projects), as necessary.
- **Legacy IT Policy Review: Usernames and Passwords**
    - Discussion:
        - Chair proposed that the development team (team) identify minimum criteria for Statewide Information Security Policies, in order to carry out the tasking from the State CIO to review the "legacy IT policies".
            - Criteria: The team identified the following criteria:
                - Statewide IT Security Policies must comply with State Statutes.
                    - Rationale: Policies cannot exceed statutory authority.
                - Statewide IT Security Policies must be broadly applicable to all covered entities.
                    - Rationale: Policies that are two narrow or prescriptive will not work for large portions of stakeholders and would thus result in many exception requests and/or violations and negate any actual benefit from the Policies.
                - Statewide IT Security Policies must align and address NIST Control Families at a Strategic level
                    - Rationale: Policies at this level, must align with NIST Control Families in order to guide the State as a whole toward the common information security framework, required by the Statewide Policy: Information Security Programs.
        - Review: Next the team applied this criteria to the first "legacy IT policy; Usernames and Passwords (Policy)", to determine if the Policy meets these criteria:
            - Statewide IT Security Policies must comply with State Statutes.
                - Determination: Pass.
            - Statewide IT Security Policies must be broadly applicable to all covered entities.
                - Determination: Fail.
                    - The Policy is very narrow and prescriptive in its language. In addition it is not strategic in nature. Many stakeholders have requested and received exceptions to the Policy. Others are in violation of it today. This renders the Policy ineffective and mostly unenforceable on a statewide basis.
            - Statewide IT Security Policies must align and address NIST Control Families at a Strategic level
                - Determination: Fail.
                    - The Policy addresses only one possible type of "Identifier" in discussing "Usernames", and addresses only one possible type of "Authenticator" in discussing "Passwords". Thus it does not align with NIST which takes the approach of addressing the entire control family related to "Identification and Authentication", of which usernames and passwords are only two, of many, specific types of each of these controls.

- Recommendation of Development Team:
  - Of the three courses of action the development team was tasked to select from in reviewing the legacy IT policies:
    - Retain as written
    - Revise to align with NIST
    - Rescind the legacy IT policy
  - Based on the determination that the Policy failed to meet all minimum criteria to qualify as a Statewide IT Security Policy the team decided to:
    - recommend that a Statewide Standard that addresses the NIST Control Family "Identification and Authentication" be developed and published by the State CIO Policy Office. The legacy IT policy: "Usernames and Passwords", will be rescinded upon publication of the Statewide Standard: "Identification and Authentication", which will supersede it.
  - Additionally, the team decided to request that the State CIO Policy Office produce a "Statewide Guideline: Identification and Authentication" instrument, based on the NIST controls, as a companion instrument for the Standard.
- Action Item to Chair:
  - Craft and deliver decision package to the State CIO containing the above recommendations.
  - Report status of decision package to ISMG at June 24 meeting.

FUTURE ITEMS

- Next NIST Control to review, Program Management control: PM-3 "Information Security Resources"

ACTION ITEMS

- Schedule June 2010 ISMG meeting
  - ISMG Chair
- Review Key Elements of an information security program and the basic outline of an Information Security Program Plan discussed above. Does the ISMG agree on the key elements put forward by the NIST Control Family and outline in the sample Information Security Program plan?
  - If so, then the group needs to take action to adopt the key elements of an Information Security Program, and the outline of the baseline/model Information Security Program plan.
    - ISMG
  - Additionally, the group needs to determine if we should attempt to identify and further define the associated Tasks that may be required to achieve each of the Objective's in the baseline/model, Information Security Program plan.
    - ISMG
- Craft Decision Package for the State CIO, recommending creation of; "Statewide Standard: Identification and Authorization" and "Statewide Guideline: Identification and Authentication".
  - ISMG Chair
- Review legacy IT policies: Logging On and Logging Off Computer Resources and Remote Access for Employees and Contractors for action on disposition recommendation at next ISMG meeting. *(Note: the development team felt that both of these instruments could be addressed

simultaneously by the development of a "Statewide Standard: Access Controls" based on the NIST Control family: Access Controls)
    - Policy Development Team (ISMG)
- Develop a visual representation of Policy, Standard of Performance, Guideline, and Procedure taxonomy. Post to ISMG Sharepoint site. (Companion Visual to go with spreadsheet "Connect Dots Ext Req to Procedures" here: http://ent.sharepoint.mt.gov/groups/ism/ate/Policy%20Standard%20Guidelines%20Procedures%20Taxonomy/Forms/AllItems.aspx
    - ISMG Chair
- Develop a visual representation of Sample Program Implementation Strategy. Post to ISMG Sharepoint site. (Companion Visual to go with "Sample Program Implementation Strategy" document here: http://ent.sharepoint.mt.gov/groups/ism/irmp/Planning/Forms/AllItems.aspx?RootFolder=%2fgroups%2fism%2firmp%2fPlanning%2fNear%2dTerm&FolderCTID=&View=%7b9FBC1CC6%2dA447%2d4B8F%2d8F78%2d2B1E6E645E87%7d)
    - ISMG Chair

AGENDA ITEMS FOR NEXT MEETING

- Training on NIST Controls – Control Family – Program Management
    - Control PM-2 = Senior Information Security Officer. – ISMG Chair
- Adopt Key Elements of an information security program
    - ISMG
- Adopt outline of Information Security Program plan.
    - ISMG
- Determine if the ISMG should identify and define the associated Tasks that may be required to achieve each of the Objective's in the baseline/model, Information Security Program plan.
    - ISMG
- Report on Status: Decision Package for the State CIO, recommending creation of; "Statewide Standard: Identification and Authorization" and "Statewide Guideline: Identification and Authentication"
    - ISMG Chair
- Determine recommendation on legacy IT policies*: Logging On and Logging Off Computer Resources and Remote Access for Employees and Contractors *(Note: the development team felt that both of these instruments could be addressed simultaneously by the development of a "Statewide Standard: Access Controls" based on the NIST Control family: Access Controls)
    - Development Team (ISMG)